# PCI DSS 3.0 Compliance Report

AP Network:alsochlu-fap-s 2015-10-26 14:17:38

Access Points in CDE 1

Result ✗ Fail (1 violation)

| Requirement | Description | Compliance |
|---|---|---|
| 1.2.3 | Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment. | ✔ Yes |

All SSIDs are in CDE.

| CDE SSIDs | | non-CDE SSIDs |
|---|---|---|
| fortiap-s4guest | fortiap-s4intern | *No Data* |
| fortiap-s4local | | |

| Requirement | Description | Compliance |
|---|---|---|
| 2.1.1 | For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. | ✔ Yes |

Fortinet does not ship FortiAPs with default wireless encryption keys, passwords, or SNMP community strings.

| Requirement | Description | Compliance |
|---|---|---|
| 4.1.1 | Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission. | ✗ No |

The following CDE SSIDs do not have strong encryption enabled. Enable WPA2-Personal, WPA2-Enterprise, FortiCloud Captive Portal or My Captive Portal with My Radius Server or FortiCloud Authentication on each SSID below.

| SSID | Authentication |
|---|---|
| fortiap-s4guest | Open |
| fortiap-s4intern | WPA2-Personal |
| fortiap-s4local | WPA2-Enterprise |

| Requirement | Description | Compliance |
|---|---|---|
| 6.2 | Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor- supplied security patches. Install critical security patches within one month of release. | ✔ Yes |

All wireless access points are running the latest firmware.

| Access Point | CDE SSIDs | Installed Firmware | Latest Firmware |
|---|---|---|---|
| PS323C3U15000216 | fortiap-s4guest<br>fortiap-s4intern<br>fortiap-s4local | PS323C-v5.4-build0121 | PS323C-v5.4-build0121 |

| Requirement | Description | Compliance |
|---|---|---|
| 7.2 | Establish an access control system for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. | ✔ Yes |

The following is a list of users that have access to the network:

| Email | User Name | Role | Status |
|---|---|---|---|
| andrea.soliva@also.com | Andrea Soliva | admin | ✔ Active |
| pirmin.roos@also.com | roospi | guestManager | ✔ Active |

| Requirement | Description | Compliance |
|---|---|---|
| 8.1.1 | Assign all users a unique ID before allowing them to access system components or cardholder data. | ✔ Yes |

All users are assigned a unique ID.

| Requirement | Description | Compliance |
|---|---|---|
| 8.1.2 | Control addition, deletion, and modification of user IDs, credentials, and other identifier objects. | ✔ Yes |

Only administrators can add, delete, or modify user IDs, credentials, and other identifier objects.

| Requirement | Description | Compliance |
|---|---|---|
| 8.1.3 | Immediately revoke access for any terminated users. | ✔ Yes |

All system accounts are current; no terminated employees have an active system account.

| Requirement | Description | Compliance |
|---|---|---|
| 8.1.4 | Remove/disable inactive user accounts at least every 90 days. | ✔ Yes |

All system accounts are current; there are no inactive accounts on the system.

| Requirement | Description | Compliance |
|---|---|---|
| 8.1.5 | Manage IDs used by vendors to access, support, or maintain system components via remote access as follows: enabled only during the time period needed and disabled when not in use; and monitored when in use.<br>Accounts used by vendors for remote maintenance are terminated after the time period needed. | ✔ Yes |
| 8.1.8 | If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.<br>Users are logged out after 15 minutes of inactivity. | ✔ Yes |
| 8.2 | In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: passwords, token devices or smart cards, biometrics.<br>Passwords are required for all users. | ✔ Yes |
| 8.2.1 | Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.<br>All user passwords are encrypted. | ✔ Yes |
| 8.2.2 | Verify user identity before modifying any authentication credential-for example, performing password resets, provisioning new tokens, or generating new keys.<br>All password resets are sent by email to verify user identity. | ✔ Yes |
| 8.2.6 | Set passwords/phrases for first- time use and upon reset to a unique value for each user, and change immediately after the first use.<br>First-time passwords are unique and must be changed after the first use. | ✔ Yes |
| 8.5 | Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: generic user IDs are disabled or removed; shared user IDs do not exist for system administration and other critical functions; and shared and generic user IDs are not used to administer any system components.<br>No group or shared accounts are used. | ✔ Yes |
| 9.1.3 | Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.<br>Wireless access points are physically secure. | ✔ Yes |
| 10.1 | Implement audit trails to link all access to system components to each individual user.<br>All sessions are tracked in the event logs. | ✔ Yes |
| 11.1 | Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis. Note: Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS. Whichever methods are used, they must be sufficient to detect and identify both authorized and unauthorized devices.<br>All Access Points in CDE have the rogue AP detection enabled. | ✔ Yes |
| 11.4 | Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.<br>Intrusion-detection is not enabled. | ✔ Yes |

| Access Point | CDE SSIDs | Platform Profile | Rogue AP Detection |
|---|---|---|---|
| PS323C3U15000216 | fortiap-s4guest<br>fortiap-s4intern<br>fortiap-s4local | alsochlu-demo-room | Enabled |

# Rogue Access Point Scanning Result

AP Network:alsochlu-fap-s 2015-10-26 14:17:38

| SSID | MAC Address | State | Vendor | Detected By | Security | Last Seen |
|---|---|---|---|---|---|---|
| | 00:18:0a:22:5a:fd | Unclassified | Meraki, Inc. | PS323C3U15000216 | WPA/WPA2 Personal | 8h ago |
| | 20:bb:c0:5b:cc:1e | Unclassified | Cisco | PS323C3U15000216 | WPA2 Personal | 8h ago |
| | 32:09:0f:f9:29:29 | Unclassified | Fortinet Inc. | PS323C3U15000216 | OPEN | 8h ago |
| | 58:97:1e:b3:4c:75 | Unclassified | Cisco | PS323C3U15000216 | WPA2 Personal | 8h ago |
| | 84:78:ac:8d:82:82 | Unclassified | Cisco | PS323C3U15000216 | WPA/WPA2 Personal | 8h ago |
| | 84:78:ac:8d:82:84 | Unclassified | Cisco | PS323C3U15000216 | WPA/WPA2 Enterprise | 8h ago |
| | 84:78:ac:8d:82:85 | Unclassified | Cisco | PS323C3U15000216 | WPA2 Personal | 8h ago |
| | 84:78:ac:8d:82:8a | Unclassified | Cisco | PS323C3U15000216 | WPA2 Personal | 8h ago |
| | 84:78:ac:99:ca:5d | Unclassified | Cisco | PS323C3U15000216 | WPA/WPA2 Personal | 8h ago |
| | 84:78:ac:99:ca:5e | Unclassified | Cisco | PS323C3U15000216 | OPEN | 8h ago |
| ALSO_corp | 20:bb:c0:5b:cc:13 | Unclassified | Cisco | PS323C3U15000216 | WPA2 Enterprise | 8h ago |
| ALSO_corp | 58:97:1e:b3:4c:70 | Unclassified | Cisco | PS323C3U15000216 | WPA2 Enterprise | 8h ago |
| ALSO_corp | 84:78:ac:8d:82:8f | Unclassified | Cisco | PS323C3U15000216 | WPA2 Enterprise | 8h ago |
| ALSO_Guest_test | 20:bb:c0:5b:cc:1b | Unclassified | Cisco | PS323C3U15000216 | OPEN | 8h ago |
| ALSO_guests | 20:bb:c0:5b:cc:1d | Unclassified | Cisco | PS323C3U15000216 | OPEN | 8h ago |
| ALSO_guests | 84:78:ac:c1:f0:57 | Unclassified | Cisco | PS323C3U15000216 | OPEN | 8h ago |
| ALSO_internal | 20:bb:c0:5b:cc:10 | Unclassified | Cisco | PS323C3U15000216 | WPA/WPA2 Enterprise | 8h ago |
| ALSO_internal | 84:78:ac:8d:82:8c | Unclassified | Cisco | PS323C3U15000216 | WPA/WPA2 Enterprise | 8h ago |
| only4dmz | 22:09:0f:f9:29:22 | Unclassified | Fortinet Inc. | PS323C3U15000216 | OPEN | 8h ago |
| only4dmz | 22:09:0f:f9:29:29 | Unclassified | Fortinet Inc. | PS323C3U15000216 | OPEN | 8h ago |
| s_auth | 00:1a:8c:8b:2a:8a | Unclassified | Sophos Ltd | PS323C3U15000216 | WPA2 Enterprise | 8h ago |